Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] A method for facilitating the sharing of data pertinent to a user system between a first domain and a second domain, wherein said second domain is in a session with said user system, the method comprising:
establishing a network session between said user system and said second domain, wherein said session is at least one of secure or non-secure, and wherein said second domain and said first domain are configured to interactively communicate with each other;
receiving a request from said user system to said second domain for a resource, wherein access to said resource includes authorization by said first domain;
determining the presence of at least one secure token in a cookie set by said second domain on said user system, wherein said secure token originates with said first domain and relates at least to an authorization of said user system to access said resource;
determining the validity of said secure token, if said secure token is present;
redirecting said request to said first domain, if said secure token is not present; and
if said secure token is present, and is valid, incorporat-

ing said secure token in a request to said first domain to keep the state of the session between said user system and said first domain as active.

[c2] The method of claim 1, wherein said secure token is encrypted, and is clarified by at least one of said first domain and second domain prior to its use in said request to maintain the session between said user system and said first domain.

[c3] The method of claim 1, wherein said secure token is obfuscated, and is clarified by at least one of said first domain and second domain prior to its use in said request to maintain the session between said user system and said first domain.

[c4] The method of claim 1, further comprising determining an elapsed time since the prior use of said secure token in said request to maintain the session between said user system and said first domain, and if such elapsed time is greater than a pre-defined threshold, redirecting said user system to said first domain.

[c5] The method of claim 1, further comprising using said secure token, if such secure token is present, and is valid, to fulfill said request made by said user system for said resource.

[c6] The method of claim 1, further comprising determining whether said request made by said user system is for a secure or a non-secure resource, and if said request is for a non-secure resource, fulfilling said request.

[c7] A computer system for facilitating the sharing of data pertinent to a user system between a first domain and a second domain, wherein said second domain is in a session with said user system, comprising:
a module configured to establish a network session between said user system and said second domain, wherein said session is at least one of secure or non-secure;
a module configured to establish interactive communication between said first domain and said second domain;
a module configured to receive a request made by said user system to said second domain for a resource, wherein access to said resource includes authorization by said first domain;
a module configured to substantially determine the presence of at least one secure token in a cookie set by said second domain on said user system, wherein said secure token originates with said first domain and relates at least to an authorization of said user system to access said resource;
a module configured to substantially determine the validity of said secure token, , if said secure token is

present;

a module configured to redirect said request to said first domain, if said secure token is not present; and

if said secure token is present, and is valid, a module configured to use said secure token in a request to said first domain to keep the state of the session between said user system and said first domain as active.

[c8] The system of claim 7, further comprising a module to clarify said secure token, where said secure token is obfuscated, prior to its use in said request to said first domain to keep the state of the session between said user system and said first domain as active.

[c9] The system of claim 7, further comprising a module to decrypt said secure token, where said secure token is encrypted, prior to its use in said request to said first domain to keep the state of the session between said user system and said first domain as active.

[c10] The system of claim 7, further comprising a module configured to substantially determine an elapsed time since the prior use of said secure token in said request to said first domain to keep the state of the session between said user system and said first domain as active, and if such elapsed time is greater than a pre-defined threshold, to redirect said user system to said first domain.

[c11] The system of claim 7, further comprising a module configured to use said secure token, if such secure token is present, and is valid, to fulfill said request for said resource.

[c12] The system of claim 7, further comprising a module configured to substantially determine whether said request is for a secure or a non-secure resource, and if said request is for a non-secure resource, fulfilling said request.

[c13] A method for facilitating the sharing of data pertinent to a user system between a first domain and a second domain, wherein said second domain is in a session with said user system, the method comprising:
establishing a network session between said user system and said second domain, wherein said session is at least one of secure or non-secure, and wherein said second domain and said first domain are configured to interactively communicate with each other;
receiving, on redirect from said second domain, a request made by said user system to said second domain for a resource, wherein access to said resource includes authorization by said first domain;
determining the presence of at least one user token in a cookie set by said first domain on said user system,

wherein said user token originates with said first domain and relates at least to a log-on of said user system to said first domain;
determining the validity of said user token, if said user token is present;
if said user token is at least one of not present and not valid, said user system logging-on, and, upon valid log-on, setting a user token in a cookie on said user system, which user token relates at least to said log-on; and
if said user token is present, and said user token is valid, including a secure token in said first domain response to said redirect from said second domain, wherein said secure token relates to the authorization of said user system to request said resource.

[c14] The method of claim 13, wherein said secure token included in said first domain"s response to said redirect from said second domain is obfuscated.

[c15] The method of claim 13, wherein said secure token included in said first domain"s response to said redirect from said second domain is encrypted.

[c16] The method of claim 13, further comprising:
receiving a request from said second domain, wherein said request is to keep the state of the session between said user system and said first domain as active;

determining whether said request made by said second domain contains said secure token; and
if said secure token is present, and is valid, setting the state of the session between said first domain and said user system as active.

[c17] The method of claim 13, further comprising determining whether said request made by said user system is for a secure or a non-secure resource, and if said request is for a non-secure resource, including a secure token in said first domain"s response to said redirect from said second domain authorizing fulfilling said request whether or not said user token is present.

[c18] A computer system for facilitating the sharing of data pertinent to a user system between a first domain and a second domain, wherein said second domain is in a session with said user system, comprising:
a module configured to establish a network session between said user system and said first domain, wherein said session is at least one of secure and non-secure;
a module configured to facilitate interactive communication between said first domain and said second domain;
a module configured to receive, on redirect from said second domain, a request made by said user system to said second domain for a resource, wherein access to said resource includes authorization by said first do-

main;

a module configured to substantially determine the presence of at least one user token in a cookie set by said first domain on said user system, wherein said user token originates with said first domain and relates at least to a log-on of said user system to said first domain;

a module configured to substantially determine the validity of said user token, if said user token is present;

if said user token is at least one of not present and not valid, said user system logging-on, and, upon valid log-on, setting a user token in a cookie on said user system, which token relates at least to said log-on; and

if said user token is present, and is valid, a module configured to include a secure token in said first domain's response to said redirect from said second domain, wherein said secure token relates to the authorization of said user system to request said resource.

[c19] The system of claim 18, further comprising a module to obfuscate said secure token prior to inclusion in said first domain"s response to said redirect from said second domain.

[c20] The system of claim 18, further comprising a module to encrypt said secure token prior to inclusion in said first domain"s response to said redirect from said second do-

main.

[c21] The system of claim 18, further comprising:
a module to receive a request from said second domain, wherein said request is to keep the state of the session between said first domain and said user system as active;
a module to substantially determine whether said request contains said secure token; and
if said secure token is present in said request, and said token is valid, setting the state of said session between said first domain and said user system as active.

[c22] A secure token comprising computer readable program code relating at least to the authorization of a user system in a session with a second domain, which session is one of secure or non-secure, to access a resource, wherein access to said resource includes authorization by a first domain, and wherein said computer readable program code derives from a secure token included by said first domain in a response to a redirect by said second domain of a request for said resource, which secure token is included in a cookie set by the second domain on the user system, and wherein said secure token is associated with a user token in a cookie set by said first domain on said user system at log-on to said first domain.

[c23] The secure token of claim 22, wherein said secure token is obfuscated by said first domain prior to inclusion in said first domain"s response to said redirect from said second domain.

[c24] The secure token of claim 22, wherein said secure token is encrypted by said first domain prior to inclusion in said first domain"s response to said redirect from said second domain.

[c25] A method for facilitating the sharing of data pertinent to a user system between a first domain and a second domain, wherein said second domain is in a session with said user system, the method comprising:
establishing a network session between said user system and said second domain, wherein said session is at least one of secure or non-secure, and wherein said second domain and said first domain are configured to interactively communicate with each other;
receiving a request from said user system to said second domain for a resource, wherein access to said resource includes authorization by said first domain;
requesting, by said second domain, authentication of said user session at said first domain;
determining the validity of said authentication, if said authentication is present;

redirecting said request to said first domain, if said authentication is not valid; and

if said authentication is valid, maintaining the state of the session between said user system and said first domain as active.